

# Novell Advanced X509 Login Method for NMAS

3.x

www.novell.com

QUICK START

## Installing and Using Advanced X509

The Advanced X509 login method for NMAS™ enables you to authenticate to eDirectory using a trusted root certificate to verify the subject name and/or alternate subject name in a user certificate. This is similar to other login methods provided for use with NMAS.

### INSTALLING AND CONFIGURING THE LOGIN METHOD FOR ADVANCED X509

Information for installing and configuring the login method is provided here. For additional information, including how to create and authorize login sequences, see the NMAS Administration Guide at the Novell Documentation [Web site \(http://www.novell.com/documentation/nmas30/index.html\)](http://www.novell.com/documentation/nmas30/index.html).

### Prerequisites

You must meet the following prerequisites before installing Advanced X509:

- ◆ NMAS Client 2.7 (ships with Novell Client for Windows version 4.9) or later
- ◆ NMAS 2.3.x or later

### Steps

As with all login methods, you must complete the following steps to make the login method available for use:

- 1 Set up any required hardware.
- 2 Install the login method.
- 3 Configure the login method.
- 4 Create a login sequence.
- 5 Authorize login sequences for users.

### Setting Up the Hardware

The Advanced X509 login method does not require any additional hardware.

**Novell**®

## Installing the Login Method for Advanced X509

There are two steps in installing and setting up the login method for Advanced X509:

1. Set up the login method in Novell eDirectory™.
2. Install the Advanced X509 client module on each workstation.

### Setting Up the Login Method in eDirectory

There are three ways to set up the login method in eDirectory.

- ♦ The Login Method Installer (Windows)

The login method installer (methodinstaller.exe) is a stand-alone utility that installs login methods into eDirectory.

- ♦ nmasinst utility (UNIX)

The nmasinst utility allows you to install login methods into eDirectory from a UNIX machine. The nmasinst utility is located in the \USR\BIN\NMASINST directory.

For information on setting up a login method using the login method installer or the nmasinst utility, see the [NMA3 Administration Guide \(http://www.novell.com/documentation/nmas30/index.html\)](http://www.novell.com/documentation/nmas30/index.html).

- ♦ ConsoleOne (Windows)

**IMPORTANT:** Run ConsoleOne® from a Windows\* client workstation by using the ConsoleOne executable located on the server at *server:SYS\PUBLIC\MGMT\CONSOLEONE\1.2\BIN\CONSOLEONE.EXE*.

- 1 In ConsoleOne, expand the Security container.
- 2 Right-click the Authorized Login Methods container.
- 3 Select New > Object.
- 4 The New Object Wizard starts.
- 5 Select the SAS:NMA3 Login Method class > click OK.
- 6 Specify the configuration file > click Next.

The configuration file is located in the login method folder and is usually named CONFIG.TXT.

- 7 From the license agreement screen, click Accept > Next.
- 8 Accept the default method name or rename it > click Next.
- 9 Review the available modules for this method > click Next.
- 10 If you want a login sequence to only use this login method, check the appropriate check box > click Finish.

11 Review the installation summary > click OK.

12 If necessary, close and restart ConsoleOne to run the newly installed ConsoleOne login method snapins. You can then configure the login method and enroll users to use it.

#### Installing the Advanced X509 Client Module on Each Workstation

The client module must be installed on each workstation that will use the Advanced X509 login method.

To install the client module, run `clientsetup.exe` in the `advx509\client` directory on each workstation that will use the login method. Follow the instructions of the installation wizard.

#### Configuring the Login Method for Advanced X509

After the login method for Advanced X509 is installed, you can manage it using ConsoleOne.

To configure this login method, you will need to do two levels of configuration:

- ♦ General Method configuration
- ♦ User Object configuration

#### General Method Configuration

1 In ConsoleOne, expand the Security container.

2 Right-click the Organizational CA > Properties > Certificates > Self Signed Certificate > Export.

This opens the Export wizard. Follow the instructions of the wizard to export the Organizational CA's self signed certificate.

**NOTE:** Do not export the private key. Also, export the certificate in der format.

3 Create a new trusted root container under the Security container by right-clicking the Security container and selecting New > Object.

The New Object Wizard starts.

4 Select the NDSPKI:Trusted Root class and click OK.

5 Enter a name for the trusted root container and click OK.

6 Create a trusted root object in the trusted root container by right-clicking the trusted root container and selecting New > Object.

The New Object Wizard starts.

7 Select the NDSPKI:Trusted Root Object class and click OK.

8 Enter a name for the trusted root object and click OK.

9 Browse for the Organizational CA's self signed certificate you exported in step 2., select it,

and click Finish.

- 10 Expand the Authorized Login Method, right-click the X509 Advanced Certificate object, and click Properties > Certificate tab.
- 11 Add the new trusted root container as a Certificate Search container by clicking Add. Browse for the trusted root container, select it, and click OK > OK.

#### User Object Configuration

- 1 Double-click a User object.
- 2 Click the Security tab > Certificates.
- 3 Create a User certificate.
- 4 Click Export and select the User certificate.

**IMPORTANT:** Make sure you check the box to export the certificate's private key.

- 5 Double-click the User object again.
- 6 Click the Security tab > Certificate Subject Names.
- 7 Click Add and type in either the User object's subject name or an alternate subject name, such as the e-mail ID. Click OK.

#### Create a Login Sequence

See Chapter 2 of the NMAS Administration Guide for information on creating a login sequence.

#### Authorize Login Sequences for Users

See Chapter 2 of the NMAS Administration Guide for information on authorizing a login sequence for users.

Copyright © 2005 Novell, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher. Novell, ConsoleOne and eDirectory are registered trademarks of Novell, Inc. in the United States and other countries. NMAS and Novell Modular Authentication Service are trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners. A trademark symbol (® , TM, etc.) denotes a Novell trademark; an asterisk (\*) denotes a third-party trademark.